JOURNAL OF COMPUTER AND SYSTEM SCIENCES 24, 1–14 (1982)

Computing Lower Bounds on Tensor Rank over Finite Fields

SHARON J. LASKOWSKI*

Department of Computer Science, The Pennsylvania State University, University Park, Pennsylvania 16802

Received August 6, 1980; revised April 4, 1981

A lower bound on rank is constructed for arbitrary tensors over finite fields. For fields of low cardinality the bound is more precise than those generated by previously known techniques because the structure of the field is exploited. In addition, the proof technique over Z_2 leads to a method for determining whether the lower bound constructed also represents an upper bound and, hence, the rank. As an application of this idea, it is shown that eight multiplications are necessary and sufficient to calculate the four-dimensional quaternion product over Z_2.

1. INTRODUCTION

Arithmetic complexity is concerned with determining the number of arithmetic operations required to solve an algebraic problem. One class of problems that has received considerable attention is that of evaluating a set of bilinear forms. In particular, the number of multiplications required by such problems as the multiplication of matrices, polynomials, etc., has been studied by many researchers [2, 12–15].

The rank of a three-dimensional tensor has been used extensively as a model for obtaining bounds on the complexity of these problems. (See, for example, [3, 8, 10].) It has been show that calculating the rank of a tensor is equivalent to finding the minimum number of nonscalar multiplications needed by the problem the tensor represents. We choose the tensor notation as described in Section 2 since it is a convenient way of presenting our lower bound technique which is based on previous work by the author in [10, 11].

Various lower bound arguments have been developed for bilinear multiplication problems. Substitution and linear independence techniques as in [2] have predominated. Partitioning [3, 4], which is a combination of linear independence and substitution, has yielded some lower bounds based on the tensor model.

All of these arguments apply to multiplication problems as viewed over an arbitrary field. Obviously, there exist fields over which a problem may require very few multiplications. In particular, a field of high cardinality may allow a reduction in

* This reasearch was supported in part by NSF Grants MCS-80-02681, and MCS-79-03428.

0022-0000/82/010001-14$02.00/0

the number of multiplications needed over one of lower cardinality [7, 8]. As a result, the lower bounds generated are often imprecise for finite fields, since the techniques cannot take advantage of the additional structure of the field.

We will present a lower bound argument that allows greater precision over finite fields. In fact, we will demonstrate how to calculate a lower bound explicitly for an arbitrary size m by p by q tensor over a finite field Z_t, where t is prime. In addition, we will show how one of our proof techniques can aid in generating actual algorithms meeting the bounds.

2. Terminology

We will now formally define tensor rank using the notation standard in the literature [3, 4] and describe how it relates to bilinear form multiplication problems.

An m by p by q *tensor* is a set of m, p by q matrices $\{G_i\}$, $1 \leqslant i \leqslant m$, over a commutative ring K. This set can be characterized by a matrix polynomial $G(s)$ in m indeterminates:

$$G(s) = \sum_{i=1}^{m} s_i G_i.$$

Each G_i can be expressed as a sum

$$\sum_{k=1}^{\delta} a_{ik} b_k c_k^T,$$

where $a_{ik} \in K$ and b_k, c_k are vectors of lengths p and q, respectively, with components in K.

Each $\sum_{i=1}^{m} s_i a_{ik} b_k c_k^T$ is a "rank-one tensor" or *dyad*. The minimum number of dyads, δ, needed to represent $G(s)$ is the *rank*. This rank is equivalent to the number of nonscalar multiplications needed to calculate the m bilinear forms $x^T G_i y$, $1 \leqslant i \leqslant m$, with $x = (x_1, x_2, ..., x_p)$ and $y = (y_1, y_2, ..., y_q)$. (See [3].)

For example, to calculate $(p_0 + p_1 x)(q_0 + q_1 x)$ over Z_2, we must compute the sums of products:

$$p_0 q_0,\ (p_0 q_1 + p_1 q_0),\ p_1 q_1.$$

The naive method requires four nonscalar multiplications, but the following computation requires only three:

$$p_0 q_0,\ (p_0 + q_1)(q_0 + q_1) + p_0 q_0 + p_1 q_1,\ p_1 q_1.$$

In our tensor representation, we associate each sum of products with a plane of the tensor and introduce indeterminates s_1, s_2 and s_3 to distinguish between G_1, G_2 and G_3 as follows:

$$p_0q_0 \sim \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix},$$

$$p_0q_1 + p_1q_0 \sim \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

$$p_1q_1 \sim \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix},$$

$$G(s) = s_1 \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + s_2 \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} + s_3 \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} s_1 & s_2 \\ s_2 & s_3 \end{bmatrix}.$$

This can be rewritten with dyads as:

$$G(s) = (s_1 + s_2) \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + s_2 \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} + (s_3 + s_2) \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

In other words, if the above expression is minimal, $G(s)$ has rank equal to 3. A simple instance of our lower bound theorem will show that the rank of $G(s)$ is indeed 3 over Z_2.

3. Lower Bounds Using Algebraic Coding Theory

We will first present a special case of the lower bound theorem and show how it can be used to generate a new lower bound for quaternion multiplication over Z_2.

The technique developed in the proof of the theorem over Z_2 can be useful in constructing the dyads representing an algorithm for the problem, as we will see in the example. In order to present the proof we need some terminology borrowed from algebraic coding theory [1, 4].

Let v_i, $1 \leqslant i \leqslant m$, be $\{0, 1\}$ − vectors and "+" be the exclusive *OR*. The *Hamming norm* (the number of 1's in a v_i) is denoted by $|v_i|$. A *code* is a set of v_i's all of the same length.

Given an m by p by q tensor $G(s)$ along with δ dyads summing to $G(s)$, we can construct a code for these dyads as follows: Let the code consist of m vectors v_i, $1 \leqslant i \leqslant m$, each of length δ such that:

$$(v_i)_j = 1 \qquad \text{if the } j\text{th dyad includes } s_i,$$
$$= 0 \qquad \text{if not.}$$

If we have only $G(s)$ and not the dyads, we can still describe to some extent what the code must look like based on the matrix ranks of the G_i's. Suppose that $G_{i_1} + G_{i_2} + \cdots + G_{i_n}$, $1 \leqslant i_j$, $n \leqslant m$, has rank k (recalling that G_{i_j} has a 1 whenever an s_{i_j} occurs in the tensor), then $|v_{i_1} + v_{i_2} + \cdots + v_{i_n}|$ must be $\geqslant k$. If not, then there would be s_i's occurring in $<k$ dyads, and the rank of $G_{i_1} + \cdots + G_{i_n}$, $n \leqslant m$, would be

$<k$, which is a contradiction. The set of inequalities on these Hamming norms of all possible exclusive *OR* sums of the v_i's is called the set of *constraints* of $G(s)$.

For example, given a code of two vectors v_1 and v_2, the possible sums are v_1, v_2, $v_1 + v_2$. The constraints based on the corresponding say, G_1, G_2, and $G_1 + G_2$ are

$$|v_1| \geqslant r(G_1), |v_2| \geqslant r(G_2), |v_1 + v_2| \geqslant r(G_1 + G_2),$$

where $r(X)$ refers to the matrix rank of X.

The code for the dyads in the example of Section 2 is

$$\begin{aligned} v_1 &= 1 \quad 0 \quad 0 \qquad s_1, \\ v_2 &= 1 \quad 1 \quad 1 \qquad s_2, \\ v_3 &= 0 \quad 0 \quad 1 \qquad s_3. \end{aligned}$$

Each column represents the indeterminates of the respective dyads. The constraints this code must meet are

$$\begin{aligned} &|v_1| \geqslant 1, \qquad |v_1 + v_2| \geqslant 2, \qquad |v_1 + v_2 + v_3| \geqslant 1, \\ &|v_2| \geqslant 2, \qquad |v_1 + v_3| \geqslant 2, \\ &|v_3| \geqslant 1, \qquad |v_2 + v_3| \geqslant 2. \end{aligned}$$

Th columns of the codes actually represent information about how each dyad must be configured.

Given only the constraints, the minimum length code can be produced to give us the lower bound theorem over Z_2.

THEOREM 1. *Let $G(s)$ be an m by p by q tensor over Z_2.*

The rank of $G(s) \geqslant \lceil (\sum_{I \in 2^{[m]}} r(\sum_{i \in I} G_i))/2^{m-1} \rceil$, where $2^{[m]}$ is the power set of m, $r(X)$ is the matrix rank of X, and $\lceil x \rceil$ is the greatest integer $\leqslant x$.

Proof. Note the following fact: If $0 \neq w = (w_1, w_2, \ldots, w_m)$ *is a* $\{0, 1\}$-vector, then $\sum_{I \in 2^{[m]}} |\sum_{i \in I} w_i| = 2^{m-1}$. This is easy to prove by induction on m. Clearly, it is true for $m = 1$, since $|1| = 2^0$. Assume the fact is true for vectors of length m. If w is a vector of length $m + 1$, w consists of a vector of length m and a component $j \in \{0, 1\}$. Then

$$\begin{aligned} \sum_{I \in 2^{[m+1]}} \left| \sum_{i \in I} w_i \right| &= \sum_{I \in 2^{[m]}} \left| \sum_{i \in I} w_i \right| + \sum_{I \in 2^{[m]}} \left| \sum_{i \in I} w_i + j \right| \\ &= 2^{m-1} + 2^{m-1} = 2^m. \end{aligned}$$

Suppose $v_1, v_2, \ldots, v_m$ is a code for $G(s)$ of minimum length. The rank of $G(s)$ must be $\geqslant$ the minimum length code. The constraints of $G(s)$ give a lower bound on the

length and, thus, a bound on the rank. The sum of the Hamming norms of all possible sums on the v_i's is equal to the length of the code times $2^{m-1}$by the above fact. This sum must be $\geqslant$ the sum of the right sides of the inequalities making up the constraints. Therefore, $r(G(s)) \geqslant$ minimum length of the code $\geqslant$ the sum of constraints/2^{m-1}. ∎

4. An Example

We will now apply this result to generate a bound of eight multiplications for quaternion multiplication over Z_2, which is better than previously known lower bounds.

Quaternions are elements over a ring, of the form

$$X = x_1 + x_2 i + x_3 j + x_4 k,$$

where

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad \text{and} \quad ki = -ik = j.$$

The quaternion multiplication problem corresponds to computing $W = XY$ where $X = (x_1, x_2, x_3, x_4)$, $Y = (y_1, y_2, y_3, y_4)$ and is defined as the calculation of $W = (w_1, w_2, w_3, w_4)$ with

$$\begin{aligned} w_1 &= (x_1 y_1 - x_2 y_2 - x_3 y_3 - x_4 y_4), \\ w_2 &= (x_1 y_2 + x_2 y_1 + x_3 y_4 - x_4 y_3)i, \\ w_3 &= (x_1 y_3 - x_2 y_4 + x_3 y_1 + x_4 y_2)j, \\ w_4 &= (x_1 y_4 + x_2 y_3 - x_3 y_2 + x_4 y_1)k. \end{aligned}$$

Over the rational and real numbers, quaternion multiplication requires exactly eight multiplications [5, 6]. Over finite fields the best lower bound is 7 and over the integers there is an upper bound of 10. The algorithms which use eight multiplications require division in such a way that they cannot be translated to algorithms over Z or Z_2.

Over Z_2 the quaternion product can be represented by tensor:

$$Q(s) = \begin{bmatrix} s_1 & s_2 & s_3 & s_4 \\ s_2 & s_1 & s_4 & s_3 \\ s_3 & s_4 & s_1 & s_2 \\ s_4 & s_3 & s_2 & s_1 \end{bmatrix},$$

which can be ranked as follows with eight dyads:

$$Q(s) = s_2 \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} + s_3 \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} + s_4 \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

$$+ (s_1 + s_2 + s_3 + s_4) \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} + (s_1 + s_2 + s_3 + s_4) \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

$$+ (s_1 + s_2 + s_3) \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} + (s_1 + s_2 + s_4) \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

$$+ (s_1 + s_3 + s_4) \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}.$$

Through the code construction, it will be shown here that the lower bound is 8. Notice that a direct application of Theorem 1 only gives a lower bound of 6.

LEMMA 1. *The tensor*

$$Q^{12}(s) = \begin{bmatrix} s_1 & s_2 & 0 & 0 \\ s_2 & s_1 & 0 & 0 \\ 0 & 0 & s_1 & s_2 \\ 0 & 0 & s_2 & s_1 \end{bmatrix}$$

has rank $= 6$ *over* Z_2.

Proof. From the lower bound theorem the rank $\geqslant (4 + 4 + 2)/2 = 5$. The only code satisfying the constraints:

$$|v_1| \geqslant 4, \qquad |v_2| \geqslant 4, \qquad |v_1 + v_2| \geqslant 2,$$

is

$$\begin{array}{lccccc} v_1 & 1 & 1 & 1 & 1 & 0 \\ v_2 & 0 & 1 & 1 & 1 & 1 \end{array}$$

up to a permuting of the columns. Notice that one dyad must have only an s_1 indeterminate (see the first column of the code). If this dyad is removed from the tensor, it will, at most, reduce the rank of G_1 by 1. This new tensor will have rank $\geqslant [9/2] = 5$ rather than 4 as we would expect if the code actually represented a ranking. Hence, $Q^{12}(s)$ has rank 6. ∎

The next step is to add another indeterminate to the tensor and calculate its rank.

LEMMA 2. *The tensor*

$$Q^{123}(s) = \begin{bmatrix} s_1 & s_2 & s_3 & 0 \\ s_2 & s_1 & 0 & s_3 \\ s_3 & 0 & s_1 & s_2 \\ 0 & s_3 & s_2 & s_1 \end{bmatrix}$$

has rank $= 7$ *over* Z_2.

Proof. It is impossible to construct a code of length 6 for the constraints:

$$|v_i| \geqslant 4, \qquad i \neq j \in \{1, 2, 3\},$$
$$|v_i + v_j| \geqslant 2,$$
$$|v_1 + v_2 + v_3| \geqslant 4,$$

with the additional stipulation from Lemma 1 that no two v_i's represent a code of length 5 for $Q^{12}(s)$. From the constraint $|v_1 + v_2 + v_3| \geqslant 4$ it is clear that four of the columns in the code have three 1's each. If one of them had a 1 and two 0's, those two vectors with the 0's would represent a code for $Q^{12}(s)$ of length 5 which contradicts Lemma 1. Thus, the code is

$$\begin{matrix} v_1 & 1 & 1 & 1 & 1 & a_1 & b_1 \\ v_2 & 1 & 1 & 1 & 1 & a_2 & b_2 \\ v_3 & 1 & 1 & 1 & 1 & a_3 & b_3 \end{matrix}$$

If $a_1 = 0$, then $a_2 = a_3 = 1$ and $|v_2 + v_3| \leqslant 1$. If $a_1 = 1$, then $a_2 = a_3 = 0$ and $|v_2 + v_3| \leqslant 1$. Therefore, $Q^{123}(s)$ has rank 7. ∎

A typical code of length 7 for $Q^{123}(s)$ meeting the constraints *and* representing an algorithm is

$$\begin{matrix} v_1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & s_1 \\ v_2 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & s_3 \\ v_3 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & s_2 \end{matrix}$$

The dyads for $Q^{123}(s)$ whose indeterminates are represented by this code are

$$(s_1 + s_2) \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} + (s_1) \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} + (s_1 + s_2 + s_3) \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$+(s_1+s_2+s_3)\begin{bmatrix}0&0&0&0\\0&0&1&0\\0&0&1&0\\0&0&1&0\end{bmatrix}+(s_1+s_2+s_3)\begin{bmatrix}0&0&0&0\\0&0&0&0\\1&0&0&1\\0&0&0&0\end{bmatrix}$$

$$+(s_1+s_3)\begin{bmatrix}0&0&1&1\\0&0&1&1\\0&0&1&1\\0&0&1&1\end{bmatrix}+(s_3)\begin{bmatrix}0&1&0&1\\0&0&0&0\\0&0&0&0\\0&1&0&1\end{bmatrix}.$$

In fact, only 16 different codes meet these constraints as listed below:

(1)
1 1 1 1 1 1 1
1 1 1 1 1 0 0
0 1 1 1 1 1 0

(2)
1 1 1 1 1 1 1
1 1 1 1 1 0 0
0 0 1 1 1 1 0

(3)
1 1 1 1 1 1 0
0 1 1 1 1 1 1
1 1 1 1 1 0 1

(4)
1 1 1 1 1 1 0
0 1 1 1 1 1 1
0 1 1 1 1 0 0

(5)
1 1 1 1 1 1 0
0 1 1 1 1 1 1
0 1 1 1 0 0 1

(6)
1 1 1 1 1 1 0
0 0 1 1 1 1 1
1 0 1 1 1 0 1

(7)
1 1 1 1 1 1 0
0 0 1 1 1 1 1
1 0 1 1 1 0 0

(8)
1 1 1 1 1 1 0
0 0 0 1 1 1 1
1 1 0 1 1 0 0

(9)
1 1 1 1 1 1 0
0 0 1 1 1 1 0
1 0 1 1 0 0 1

(10)
1 1 1 1 1 0 0
0 0 1 1 1 1 1
1 0 1 1 1 0 1

(11)
1 1 1 1 1 0 0
0 1 1 1 1 1 0
0 1 1 1 1 0 1

(12)
1 1 1 1 1 0 0
0 0 1 1 1 1 1
1 0 1 1 0 0 1

(13)
1 1 1 1 1 0 0
0 1 1 1 1 1 0
1 0 0 1 1 0 1

(14)
1 1 1 1 1 0 0
0 1 1 1 1 1 0
0 0 1 1 1 0 1

(15)
1 1 1 1 1 0 0
0 0 1 1 1 1 0
1 0 0 1 1 0 1

(16)
1 1 1 1 0 0 0
0 0 1 1 1 1 0
1 0 1 0 0 1 1

These codes can be constructed by a brute force testing of all combinations of three {0-1}-vectors against the constraints listed in Lemma 2. For example, if v_1 is fixed with $|v_1| = 7$, then it is obvious that $4 \leqslant |v_2|, |v_3| \leqslant 5$ and that when $|v_2| = |v_3| = 4$, $|v_1 + v_2 + v_3| < 4$. Therefore, there are only two codes (up to permuting columns) that satisfy all the constraints. The same procedure can be repeated for different values of $|v_1|$. Of these codes, only (6), (7), (8), (10), (12), (14), (15) and (16) are algorithms. The others can be proved not to be valid algorithms with the following two techniques which will be presented for (1) and (2).

LEMMA 3. *There are eight codes of length 7 which represent rankings of* $Q^{123}(s)$.

Proof. We will show that codes (1)–(5), (9), (11), and (13) do not represent a set

of dyads for $Q^{123}(s)$. For code (1) associate with each column: D_1, D_2,..., D_7, each representing a rank one matrix. Now, $G_1 + G_2 = D_6 + D_7$. Then D_6 must have one of the following forms:

$$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$

or any rotation of either of these along the diagonal. Notice that $G_2 + G_3 + D_6 = D_1$. However, $G_2 + G_3 + D_6 =$

$$\begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

and

$$\begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix},$$

both of which have matrix rank > 1. Hence $G_2 + G_3 + D_6 \neq D_1$. Similarly, for any other form of D_6 the matrix rank will be >1 and the code cannot represent $Q^{123}(s)$.

The same argument will work for codes (3), (4), and (11).

For code (2) notice that $G_1 + G_2 = D_6 + D_7$ and $G_1 + G_2 + G_3 = D_3 + D_4 + D_5 + D_7$. Hence, $G_1 + G_2 + G_3 + D_7 = D_3 + D_4 + D_5$ with D_7 as described for code (1). But the $r(G_1 + G_2 + G_3 + D_7) > 3$ so code (2) cannot represent $Q^{123}(s)$.

This argument also holds for codes (5), (9) and (13). ∎

Now we are prepared to calculate the rank of the quaternion multiplication tensor.

THEOREM 2. *The tensor*

$$Q(s) = \begin{bmatrix} s_1 & s_2 & s_3 & s_4 \\ s_2 & s_1 & s_4 & s_3 \\ s_3 & s_4 & s_1 & s_2 \\ s_4 & s_3 & s_2 & s_1 \end{bmatrix}$$

has rank $= 8$ *over* Z_2.

Proof. Suppose $Q(s)$ has rank $= 7$. Then there exists a code of length 7 such that any three of the code vectors represent a set of dyads for $Q^{123}(s)$ and the following set of constraints hold true:

$$|v_i| \geqslant 4, \qquad |v_i + v_j| \geqslant 2, \qquad |v_i + v_j + v_k| \geqslant 4,$$
$$|v_1 + v_2 + v_3 + v_4| \geqslant 1, 1 \leqslant i \neq j \neq k \leqslant 4.$$

From Lemmas 1 and 2, no two vectors represent a code of length < 6 and no three represent a code of length < 7.

No combinations of four vectors from the codes in Lemma 3 for $Q^{123}(s)$ can be combined to satisfy all of the constraints.

Therefore $Q(s)$ has rank $= 8$. ∎

5. The Lower Bound Theorem over Finite Fields

We will present a slightly different method for proving a generalization of Theorem 1.

Suppose a 2 by p by q tensor $G(s)$ over Z_t, where t is prime, has rank r. The r dyads for $G(s)$ must have the form:

$$G(s) = \sum_{j=0}^{t-1} \left((s_1 + js_2) \sum_{i=1}^{u_j} D_{ji} \right) + \sum_{i=1}^{u_t} s_2 D_{ti},$$

where u_j is the number of dyads associated with $s_1 + js_2$, for $0 \leqslant j \leqslant t-1$, u_t with s_2, and $\sum_{j=0}^{t} u_i = r$. D_{ji}, D_{ti} are $\{0, 1\}$-matrices. We have used the fact that for any k in $Z_t - \{0\}$,

$$ks_1 + s_2 = k(s_1 + k^{-1}s_2).$$

to ensure that for tensors with two indeterminates over the field Z_t only $t+1$ sums of indeterminates need be considered: s_2, $s_1 + js_2$ $(j = 0,..., t-1)$. The rank of G_2 and any $G_1 + jG_2$ is less than or equal to the sum of t of the appropriate u_j's. Specifically, $r(G_2) \leqslant u_1 + u_2 + \cdots + u_{t-1} + u_t$, $r(G_1) \leqslant u_0 + u_1 + \cdots + u_{t-1}$ and, for $j > 0$, $r(G_1 + jG_2) \leqslant (\sum_{i=0}^{t} u_i) - u_k$, where $kj = t - 1 \bmod t$.

Hence, the sum of the matrix ranks $=$

$$\left(r(G_2) + \sum_{j=0}^{t-1} r(G_1 + jG_2) \right) \leqslant t(u_0 + \cdots + u_t)$$

and the rank $\geqslant$ [sum of the matrix ranks/t], where $[x]$ is the greatest integer $\leqslant x$.

Generalizing even further to produce our main theorem, a lower bound for m by p by q tensors over arbitrary Z_t can be proved:

THEOREM 3. *Let $G(s)$ be an m by p by q tensor over Z_t, where t is prime. The rank of $G(s)$ is*

$$\geqslant \left\lceil \left[\sum_{i=1}^{m} \left(\sum_{k_{i+1},\ldots,k_m=0}^{t-1} r(G_i + k_{i+1}G_{i+1} + \cdots + k_m G_m) \right) \right] \Big/ t^{m-1} \right\rceil,$$

where $r(X)$ is the rank of X.

Proof. We will use a more general form of the method in the example immediately preceding this theorem. First, we note that the possible indeterminates in the dyads have the forms

$$\begin{aligned} &s_1 + k_2 s_2 + k_3 s_3 + \cdots + k_m s_m \\ &\quad s_2 + k_3 s_3 + \cdots + k_m s_m \\ &\quad\quad s_3 + \cdots + k_m s_m \\ &\quad\quad \cdots \\ &\quad\quad \cdots \\ &\quad\quad\quad\quad s_m, \ 0 \leqslant k_1, \ldots, k_m \leqslant t-1, \end{aligned}$$

since any $k_i s_i + k_{i+1} s_{i+1} + \cdots$ can be rewritten as $k_i(s_i + k_i^{-1} k_{i+1} s_{i+1} + \cdots)$.

In order to calculate our lower bound formula, we will sum $r(G_1)$, $r(G_1 + G_2)$, $r(G_1 + 2G_2)$,... to produce an expression in terms of t, m, and the rank r of $G(s)$.

We have r dyads for $G(s)$, u_1 of them with indeterminate s_1, u_2 with $s_1 + s_2$, u_3 with $s_1 + 2s_2$,..., u_q with s_m, so that $\sum_{j=1}^{q} u_j = r$. Any value $r(G_i + k_{i+1}G_{i+1} + \cdots + k_m G_m)$, $0 \leqslant k_{i+1}, \ldots, k_m \leqslant t-1$, is $\leqslant \sum u_k$ for those u_k representing dyads with indeterminates $s_j + k'_{j+1} s_{j+1} + \cdots + k'_m s_m$, $0 \leqslant k'_{j+1}, \ldots, k'_m \leqslant t-1$, such that in mod t arithmetic,

$$k'_i + k_{i+1} k'_{i+1} + \cdots + k_m k'_m \neq 0 \qquad \text{if} \quad i \geqslant j$$

or

$$k_j + k_{j+1} k'_{j+1} + \cdots + k_m k'_m \neq 0 \qquad \text{if} \quad i < j.$$

In order to calculate an upper bound on $\sum_{i=1}^{m} (\sum_{k_{i+1},\ldots,k_m=0}^{t-1} r(G_i + k_{i+1}G_{i+1} + \cdots + k_m G_m))$, we must count each occurrence of the u_j's in this sum.

If there are u_j dyads having s_i alone as an indeterminate, then u_j occurs in the total sum each time G_i appears in any $r(G_j + k_{j+1}G_{j+1} + \cdots k_m G_m)$. In fact, G_i appears:

$t^{m-2}(t-1)$ times in $\{G_1 + k_2 G_2 + \cdots k_i G_i + \cdots + k_m G_m / 0 \leqslant k_2, \ldots, k_m \leqslant t-1\}$

$t^{m-3}(t-1)$ times in $\{G_2 + \cdots k_i G_i + \cdots + k_m G_m / 0 \leqslant k_3, \ldots, k_m \leqslant t-1\}$

$\vdots$

$t^{m-i}(t-1)$ times in $\{G_{i-1} + k_i G_i + \cdots + k_m G_m / 0 \leqslant k_i, \ldots, k_m \leqslant t-1\}$

t^{m-i} times in $\{G_i + \cdots + k_m G_m / 0 \leqslant k_{i+1}, \ldots, k_m \leqslant t-1\}$

for all choices of $k_1,\ldots, k_m$ with $k_i \neq 0$. Therefore, the total number of occurrences equals t^{m-1}.

For u_j's corresponding to dyads with indeterminates of the form $s_i + k_{i+1}s_i + \cdots + k_m s_m$ we relabel the indeterminates by replacing s_i by $s_i + (t - k_{i+1})s_{i+1} + \cdots + (t - k_m)s_m$ and $s_i + k_{i+1}s_{i+1} + \cdots + k_m s_m$ by s_i, do the same for the G_i's and then s_i occurs t^{m-1} times as before.

Therefore,

$$\sum_{i=1}^{m}\left(\sum_{k_{i+1},\ldots k_m=0}^{t-1} r(G_i + k_{i+1}G_{i+1} + \cdots + k_m G_m)\right) \leqslant t^{m-1}(u_1 + \cdots + u_q) = t^{m-1}r. \quad \blacksquare$$

We now have a lower bound on tensor rank.

6. Two Examples

To illustrate the power of Theorem 3, we will present two examples.

Example 1. Consider the 2 by n by n tensor,

$$G(s) = \begin{bmatrix} s_1 & s_2 & & & \cdots 0 \\ & s_1 & s_2 & & \vdots \\ & & \ddots & \ddots & \\ & & & s_1 & s_2 \\ s_2 & & & & s_1 \end{bmatrix}.$$

By applying any of the known lower bound techniques, we cannot obtain a lower bound better than n. In fact, over the field of complex numbers, the rank is n. However, over Z_2 our technique generates a lower bound of $\lceil (3n-1)/2 \rceil$ (exploiting the field structure). The upper bound is $3n/2$ for n even, since each pair of rows i and $i+1$, $i = 1, 3,\ldots, n-1$, has rank 3. For n odd, we first simplify $G(s)$ by adding rows 1 through $n-1$ to row n and column n to columns 1 through $n-1$ (still preserving the rank). Each pair of rows i and $i+1$, $i = 1, 3,\ldots, n-2$ has rank 3 and the last row has rank 1 for a total of $(3n-1)/2$.

Example 2. Consider the 3 by n by n tensor,

$$G(s) = \begin{bmatrix} s_1 & s_2 & s_3 & & & \cdots 0 \\ & s_1 & s_2 & s_3 & & \vdots \\ & & \ddots & & & \\ & & & s_1 & s_2 & s_3 \\ \vdots & & & & s_1 & s_2 \\ 0 \cdots & & & & & s_1 \end{bmatrix}.$$

Over finite fields of cardinality t, the theorem yields a lower bound $[((t^2+t+1)n-(t+2))/t^2]$. Other techniques produce a lower bound of $n+2$ over arbitrary fields. Moreover, for fields of cardinality $t \geqslant n$ and infinite fields, the rank is exactly $n+2$ [7].

7. Conclusions

Exploiting the structure of finite fields has led to the construction of a lower bound theorem for tensor rank. For fields with low cardinality the theorem provides an easy method of computing lower bounds more precise than those produced by previously used techniques. In addition, one of the proof techniques can also aid in computing rank over Z_2.

Acknowledgments

I would like to thank my thesis advisor, David Dobkin, for many thought-provoking discussions at Yale University and the University of Arizona and Joseph Ja'Ja' for his comments on the presentation of this research.

References

1. E. R. Berlekamp, "Algebraic Coding Theory," McGraw–Hill, New York, 1968.
2. A. Borodin and I. Munro, "The Computational Complexity of Algebraic and Numeric Problems," American Elsevier, New York, 1975.
3. R. W. Brockett and D. Dobkin, On the optimal evaluation of a set of bilinear forms, *Linear Alg. Appl.* **19** (1978), 207–235.
4. D. P. Dobkin, "On the Complexity of a Class of Arithmetic Computations," Ph.D. thesis, Harvard University, 1973. Also Department of Computer Science Research Report 23, Yale University, 1973.
5. T. D. Howell, "Tensor Rank and the Complexity of Bilinear Forms," Ph.D. thesis, Cornell University, 1976.
6. T. D. Howell and J. C. Lafon, "The Complexity of the Quaternion Product," Department of Computer Science Technical Report TR 75-245, Cornell University, 1975.
7. J. Ja'Ja', "Computations of Bilinear Forms over Finite Fields," Department of Computer Science Technical Report CS-78-03, The Pennsylvania State University, 1978.
8. J. Ja'Ja', Optimal evaluation of pairs of bilinear forms, *SIAM J. Comput.* **8** (1979), 443–462.
9. S. J. Laskowski and D. P. Dobkin, "The Structure and Rank of m by p by q Tensors: The Heuristic Approach," Department of Computer Science Research Report 130, Yale University, 1978. Also Johns Hopkins Conference on Information Sciences and Systems, 1978, pp. 173–178.
10. S. J. Laskowski, "The Heuristic Approach to Tensor Ranking," Ph.D. thesis, Yale University, 1980. Also, Department of Computer Science Technical Report CS-80-9, The Pennsylvania State University, 1980.
11. S. J. Laskowski, A lower bound on tensor rank, *in* "Proceedings, Princeton Conference on Information Sciences and Systems," 1980, pp. 465–467.
12. V. Y. Pan, New fast algorithms for matrix operations, *SIAM J. Comput.* **9** (1980), 321–342.

13. V. STRASSEN, Gaussian elimination is not optimal, *Numer. Math.* **13** (1969), 354–356.
14. V. STRASSEN, Evaluation of rational functions, *in* "Complexity of Computer Computations" (R. Miller and J. Thatcher, Eds.), pp. 1–10, Plenum, New York, 1972.
15. S. WINOGRAD, On the number of multiplications necessary to compute certain functions, *Comm. Pure Appl. Math.* **23** (1970), 165–179.